Kit Bit4id 4.0.0.4

Instalación y manual de Usuario para Windows

Bit4id Ibérica
C/ Marie Curie, 8-14
Forum Nord de Tecnología
08042 – Barcelona
España
Tel. +34 935 35 35 18
info.es@bit4id.com

Bit4id Italia
Via Coroglio, 57
Città della Scienza
80124 Napoli
Italia
Tel. +39 081 762 56 00
info.it@bit4id.com

Bit4id UK
2 London Wall Buildings
London Wall,
London EC2M 5UU
United Kingdom
Tel. +44 (0) 203 397 3166
info.uk@bit4id.com

Bit4id Perú
Avda. Olavegoya, nº 1835
Distrito Jesus Maria
Lima 11
Perú
Tel: +51 947 744 704
info.pe@bit4id.com

Oficina Lisboa
Rua Cesário Verde, 32
2790-495 Queijas (Lisboa)
Portugal
Tel .+351 914 58 30 21
info.pt@bit4id.com

Oficina Milán
Corso Vercelli, 11
20144 Milano
Italia
Tel. +39 024 547 42 59
info.it@bit4id.com

Oficina Guatemala
15 avenida, 14-09 zona 10
Oakland - 01010
Guatemala
Guatemala
Tel: +502 22 21 91 63
aor@bit4id.com

qualityaustria
SYSTEM CERTIFIED
ISO 9001:2008 No.07974/0
ISO 14001:2004 No.01608/0

IQNet
ISO 9001:2008
ISO 14001:2004
ISO 27001:2005

Sumario

Revisiones 3
Introducción 4
A quién va dirigido este documento 4
Antes de comenzar 4
Instalación 5
Instalación desatendida (para usuarios avanzados) 6
Problemas durante la instalación 6
Fin de la instalación 7
Antes de comenzar a usar el Kit Bit4id 7
Acceso a la aplicación 7
Funcionalidades 8
Tabla de funciones 8
Comprobaciones adicionales frente al mal funcionamiento 13
Comprobación de carga de certificados en el almacén de Windows 13
Comprobación de carga de certificados en el almacén de Firefox 14
Preguntas frecuentes 16
Glosario 18

Revisiones

Revisión	Fecha	Cambios	Autor
1.0	06/11/2012	Primera redacción	RLG
1.1	09/11/2012	FAQ	GSA
1.2	14/11/2012	Revisión y aprobación	RLG
1.3	19/11/2012	Adaptación para todo tipo de lectores	GSA
1.4	10/01/2013	Ampliación importación de certificados	GSA
1.5	22/10/2013	Actualización imagen “Acerca de …” del CardManager	CSC
1.6	30/01/2014	Adaptación a Windows 8 Actualización de “Funcionalidades” Creación “Comprobaciones adicionales”	JGM
1.6b	31/01/2014	Actualización “Comprobaciones adicionales”	JGM
1.7	10/07/2014	Actualización versión del Kit Bit4id	JGM

Introducción

Este manual sirve de guía para llevar a cabo de manera exitosa el proceso de instalación del Kit Bit4id para el uso de tarjetas criptográficas, y el procedimiento para acceder y usar la aplicación de gestión. El Kit Bit4id consta de los siguientes componentes:

- **Bit4id Middleware**: librerías que permiten a cualquier aplicación del Sistema Operativo operar con las tarjetas criptográficas mencionadas
- **Bit4id Card Manager**: aplicación para la gestión de la tarjeta, que permite realizar operaciones como cambio de PIN o PUK, desbloqueo de PIN, obtener información sobre la tarjeta,…

Este manual le guiará de una manera sencilla en el proceso de instalación y uso del Kit Bit4id.

A quién va dirigido este documento

- ***Usuarios finales***, que van a utilizar tarjetas con chip en entornos Windows

Antes de comenzar

Asegúrese de disponer de:

- Un lector de tarjetas estándar, compatible PC/SC que se encuentre correctamente conectado, instalado y configurado. Siga las instrucciones suministradas por el fabricante del lector para verificar su correcta instalación y funcionamiento
- Disponer de la última versión del Kit Bit4id.
- Para poder realizar la instalación, es indispensable poseer permisos de Administrador. En caso de no poseerlos la instalación será denegada.

Instalación

Descargue el instalador desde la página adecuada del Proveedor de Servicios de Certificación que le ha suministrado la tarjeta criptográfica y ejecútelo en su equipo. Si se le solicita, permita la ejecución de la aplicación.

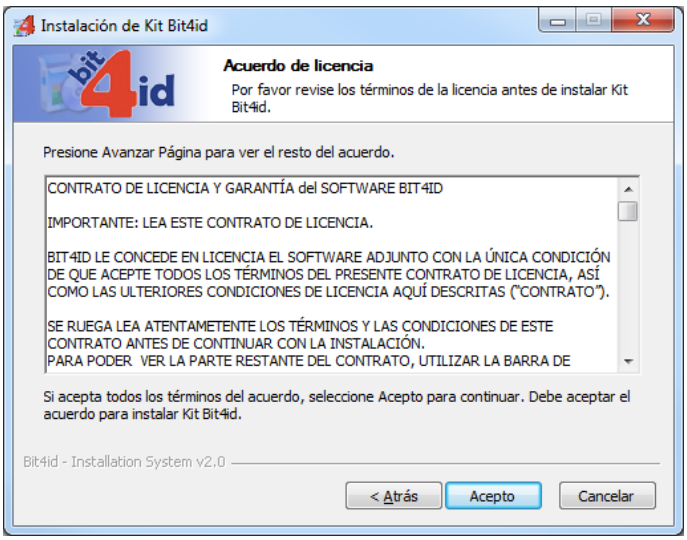
Nota: En el caso de que no le solicite la ejecución de la aplicación vaya a la carpeta de descargas, busque el icono de Kit_Bit4id y ejecútelo desde allí.

Asistente de instalación

Bienvenido al Asistente de Instalación de Kit Bit4id. Haga click en *Siguiente* para continuar.

Instalación de Kit Bit4id
Bienvenido al Asistente de Instalación de Kit Bit4id
Este programa instalará Kit Bit4id en su ordenador.
Se recomienda que cierre todas las demás aplicaciones antes de iniciar la instalación. Esto hará posible actualizar archivos relacionados con el sistema sin tener que reiniciar su ordenador.
Presione Siguiente para continuar.
Universal Middleware
Siguiente >
Cancelar

Revise los términos del acuerdo de licencia y haga click en *Acepto* para continuar


Instalación de Kit Bit4id
Acuerdo de licencia
Por favor revise los términos de la licencia antes de instalar Kit Bit4id.
Presione Avanzar Página para ver el resto del acuerdo.
CONTRATO DE LICENCIA Y GARANTÍA del SOFTWARE BIT4ID
IMPORTANTE: LEA ESTE CONTRATO DE LICENCIA.
BIT4ID LE CONCEDE EN LICENCIA EL SOFTWARE ADJUNTO CON LA ÚNICA CONDICIÓN DE QUE ACEPTE TODOS LOS TÉRMINOS DEL PRESENTE CONTRATO DE LICENCIA, ASÍ COMO LAS ULTERIORES CONDICIONES DE LICENCIA AQUÍ DESCRITAS ("CONTRATO").
SE RUEGA LEA ATENTAMETENTE LOS TÉRMINOS Y LAS CONDICIONES DE ESTE CONTRATO ANTES DE CONTINUAR CON LA INSTALACIÓN.
PARA PODER VER LA PARTE RESTANTE DEL CONTRATO, UTILIZAR LA BARRA DE
Si acepta todos los términos del acuerdo, seleccione Acepto para continuar. Debe aceptar el acuerdo para instalar Kit Bit4id.
Bit4id - Installation System v2.0
< Atrás
Acepto
Cancelar

Automáticamente se instalaran todos los componentes del Kit Bit4id.

Es necesario reiniciar el sistema para completar la instalación. Presione *Terminar* para cerrar el asistente. **Si no permite el reinicio y se continúa trabajando, se pueden producir comportamientos inesperados, por lo que no se recomienda en ningún caso.**

Instalación de Kit Bit4id
Completando el Asistente de Instalación de Kit Bit4id
Su sistema debe ser reiniciado para que pueda completarse la instalación de Kit Bit4id. ¿Desea reiniciar ahora?
Reiniciar ahora
Deseo reiniciar manualmente más tarde
Universal Middleware
< Atrás
Terminar
Cancelar

Instalación desatendida (para usuarios avanzados)

ATENCIÓN: este procedimiento es sólo para casos concretos en los que se le haya indicado explícitamente. La mayoría de usuarios no deberían realizar una instalación desatendida.

Para poder realizar una instalación desatendida basta con introducir en el cuadro de comandos el instalador pasándole como parámetro "`/S`".

ATENCIÓN: debido a las limitaciones de interacción de una instalación desatendida, es necesario eliminar versiones anteriores o incompatibles antes de proceder. Así mismo, se debe forzar el reinicio de la máquina una vez concluida la instalación.

Problemas durante la instalación

Es posible que tenga versiones anteriores de la aplicación de Gestión de la tarjeta (Bit4id Card Manager) instaladas en su equipo, por lo que se le solicitará que elimine versiones anteriores antes de ejecutar el instalador. Elimine dichas versiones y ejecute de nuevo el instalador.

Para eliminar versiones anteriores en Windows XP, diríjase al menú Inicio > Panel de control > Agregar o quitar programas > Bit4id Card Manager Admin x.x.x.x (dónde x.x.x.x representa el número de versión instalada)

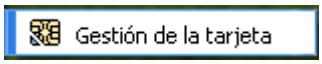
Para eliminar versiones anteriores en Windows Vista o 7, diríjase al menú Inicio > Panel de control > > Desinstalar un programa > Bit4id Card Manager Admin x.x.x.x (dónde x.x.x.x representa el número de versión instalada)

Para eliminar versiones anteriores en Windows 8, diríjase al menú lateral derecho > Configuración > Panel de control > Desinstalar un programa > Bit4id Card Manager Admin x.x.x.x (dónde x.x.x.x representa el número de versión instalada)

Fin de la instalación

Una vez finalizado el proceso de instalación se creará un acceso directo de la aplicación Bit4id Card Manager (Gestión de la tarjeta) en el escritorio que le permitirá realizar cualquier tipo de operación con la misma.

Así mismo podrá acceder a la aplicación Bit4id Card Manager a través de la sección Inicio



Antes de comenzar a usar el Kit Bit4id

Bit4id Card Manager requiere un lector de tarjetas inteligentes estándar, compatible PC/SC, que se encuentre correctamente conectado, instalado y configurado antes de comenzar.

Siga las instrucciones suministradas por el fabricante del lector para verificar su correcta instalación y funcionamiento.

Acceso a la aplicación

La aplicación Bit4id Card Manager es accesible desde el escritorio, haciendo click sobre:

Así mismo se puede acceder a la aplicación Gestión de Tarjeta a través de:

- en Windows XP, diríjase al menú Inicio > Programas > Bit4id > Gestión de la Tarjeta
- en Windows Vista o 7, diríjase al menú Inicio > Todos los programas > Bit4id > Gestión de la Tarjeta
- en Windows 8, diríjase al menú Inicio > Todas las aplicaciones > Gestión de la Tarjeta

Funcionalidades

Bit4id Card Manager (Gestión de la tarjeta) dispone de múltiples funcionalidades, accesibles desde la pantalla principal:

Tabla de funciones

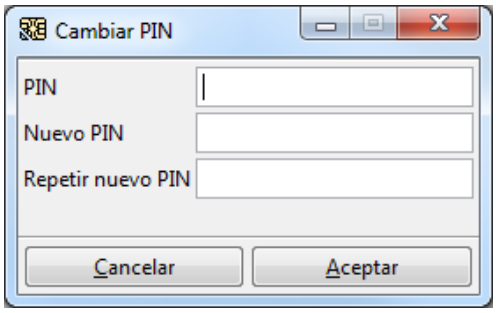
La siguiente tabla resume las funciones expuestas en la pantalla principal de Bit4id Card Manager.

Función	Descripción
Cambiar PIN	Función para cambiar el PIN de la tarjeta (ver imagen 2)
Cambiar PUK	Función para cambiar el PUK de la tarjeta (ver imagen 3)
Desbloquear PIN	Función para desbloquear el PIN de la tarjeta mediante el PUK de la misma (ver imagen 4)
Importación	Función para importar certificados a la tarjeta (ver imagen 5)
Ver…	Función para ver el listado de certificados que se encuentra en la tarjeta (ver imagen 6)
Información de la tarjeta	Ventana que muestra información sobre la tarjeta (modelo, número de serie, identificación del fabricante y etiqueta) (ver imagen 7)
Acerca de…	Función que muestra la versión instalada (ver imagen 8)

Seleccionar Lector	Función para seleccionar el lector con el que se quiere interactuar en el caso de que haya más de uno

Cambiar PIN

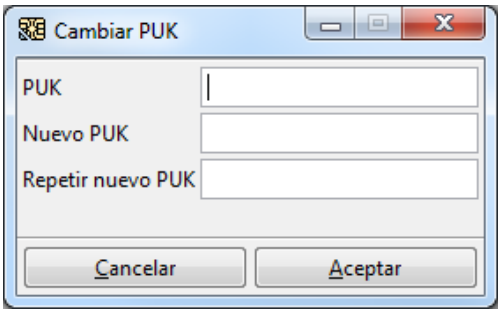
Introduzca el PIN antiguo de la tarjeta y el nuevo PIN. El nuevo PIN tiene que tener entre 6 y 8 dígitos alfanuméricos.



[Imagen 2]

Cambiar PUK

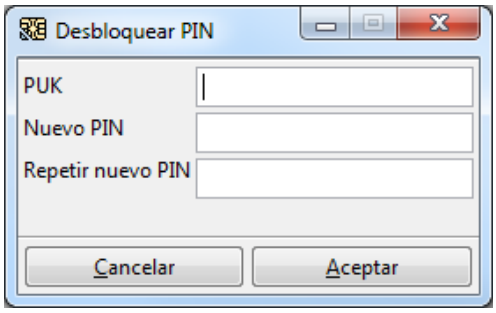
Introduzca el PUK antiguo de la tarjeta y el nuevo PUK. El nuevo PUK tiene que tener entre 6 y 8 dígitos alfanuméricos.



[Imagen 3]

Desbloquear PIN

Para desbloquear el PIN, introduzca el PUK de la tarjeta e introducir el nuevo PIN. El nuevo PIN tiene que tener entre 6 y 8 dígitos alfanuméricos.

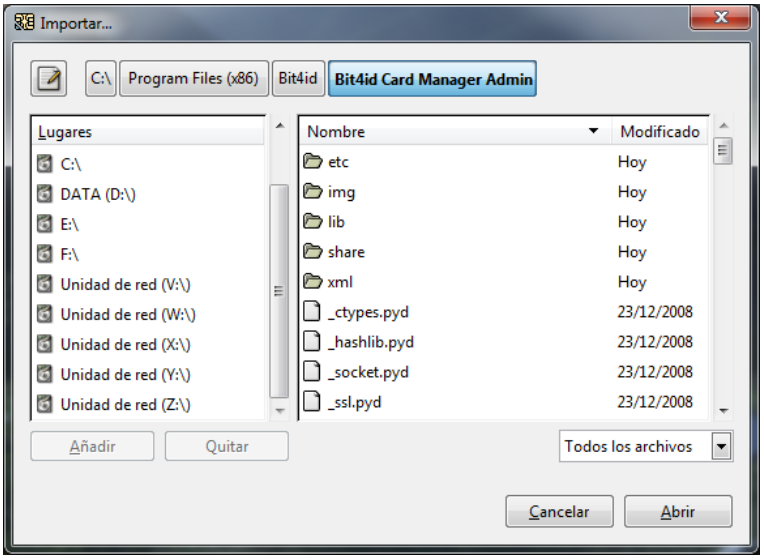


[Imagen 4]

Importación

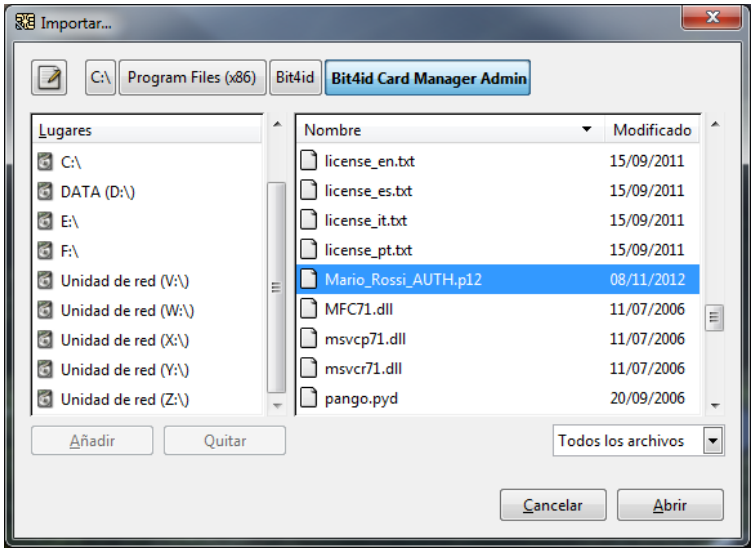
Esta opción permite la importación de certificados en la tarjeta. Los formatos aceptados para la importación de certificados en tarjeta .p12 o .pfx ya que dichos formatos incluyen la clave privada del certificado, imprescindible para realizar operaciones criptográficas.

Para iniciar la importación, antes seleccione el certificado desde su ubicación, tal y como se muestra en la siguiente imagen:



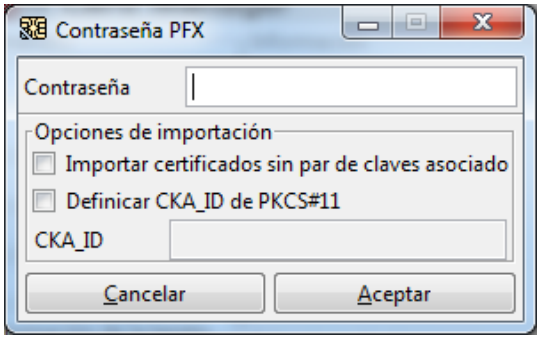
[Imagen 5]

Una vez seleccionado el certificado, presione “Abrir”:



[Imagen 5.1]

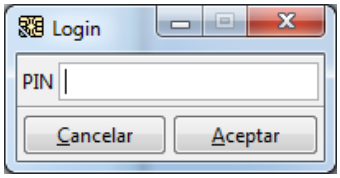
El sistema le pedirá la contraseña del archivo PFX o P12 (certificado y clave privada del mismo) que desea importar, y que contiene su certificado y par de claves. Insértela y complete según su conveniencia las opciones de importación, donde:



[Imagen 5.2]

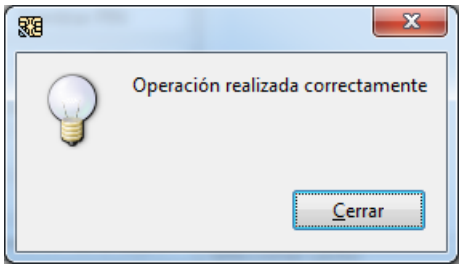
- *Importar certificados sin par de claves asociado:* permite importar toda la jerarquía de certificación incluida en el fichero PFX o P12. Recomendamos NO MARCAR esta opción.
- *Definir CKA_ID de PKCS#11:* identificador que determinadas aplicaciones utilizan a la hora de mostrar el certificado. Recomendamos introducir un valor identificativo útil, por ejemplo pedro_firma, pedro_acceso, pedro_cifrado, etc.

Una vez completado este paso, el sistema le pedirá que inserte el PIN de la tarjeta:



[Imagen 5.3]

Y la importación del certificado se habrá completado:

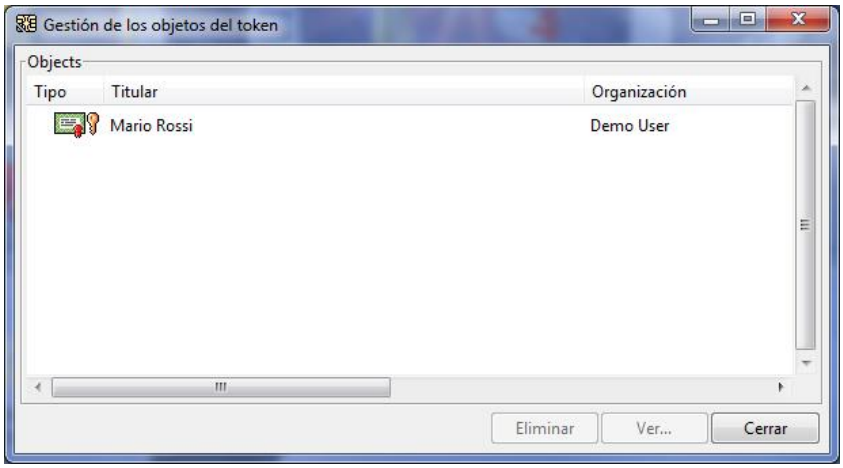


[Imagen 5.4]

En el caso que se desee comprobar que el certificado ha sido correctamente guardado, recuerde que puede revisar todos los certificados almacenados en la tarjeta a través de la opción "Ver" de Bit4id Card Manager.

Ver…

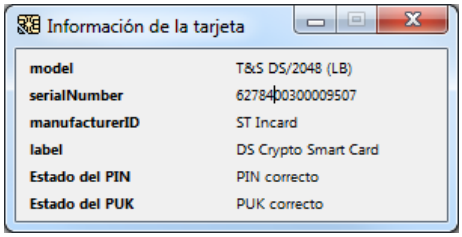
Para ver los certificados que se encuentran en la tarjeta, introduzca el PIN de la tarjeta cuando sea solicitado.



[Imagen 6]

Información de la tarjeta

Ofrece información detallada de la tarjeta: modelo, número de serie, fabricante y etiqueta.



[Imagen 7]

Acerca de…

Ventana que muestra la versión de Bit4id Card Manager (Gestión de la tarjeta).

[Imagen 8]

Comprobaciones adicionales frente al mal funcionamiento

Los resultados de las siguientes comprobaciones son necesarias para la resolución de cualquier tipo de incidencia. Dichos resultados se deben reportar al departamento técnico ante cualquier incidencia relacionada con el uso de sus certificados almacenados en sus tarjetas. De esta forma se reducirá el tiempo de resolución de la misma.

Comprobación de carga de certificados en el almacén de Windows

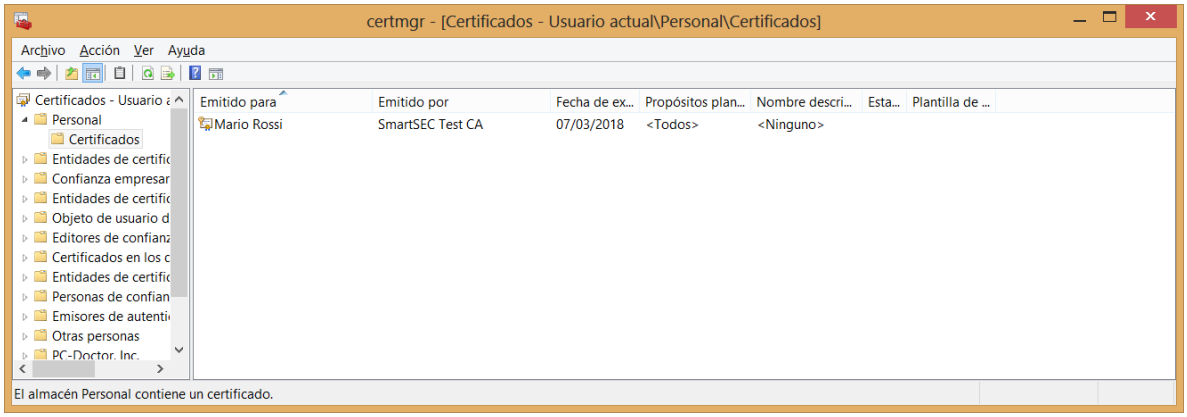
Asegúrese de disponer de:

- Lector de tarjetas conectada a la máquina
- Tarjeta inteligente insertada en el lector
- Al menos un certificado almacenado en la tarjeta

Esta prueba pretende comprobar la correcta carga de los certificados de la tarjeta en el almacén de certificados de Windows, lo cual es imprescindible para el uso de nuestros certificados en aplicaciones de Microsoft. Para ello debemos abrir dicho almacén:

- en Windows XP, diríjase al menú Inicio > Ejecutar e introduzca "*certmgr.msc*"
- en Windows Vista o 7, diríjase al menú Inicio > Buscar programar y archivos > Introduzca "*certmgr.msc*"
- en Windows 8, diríjase al menú Inicio > e introduzca *certmgr.msc*

Una vez ejecutada la ventana, abra la carpeta *Personal* y seguidamente la carpeta *Certificados* tal y como muestra la siguiente imagen:



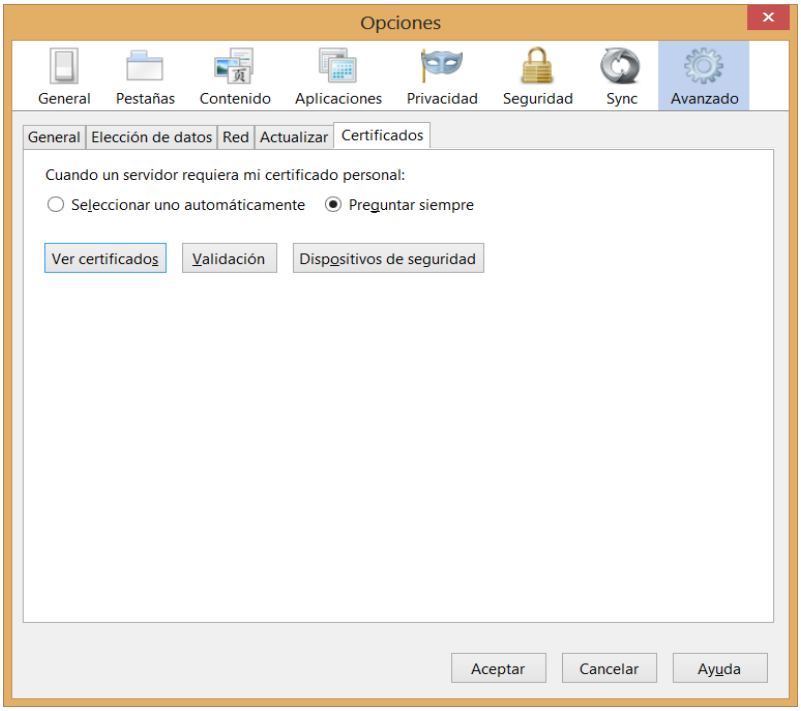
[Imagen 9]

Si se le muestra información referente a los certificados de su tarjeta la comprobación habrá finalizado satisfactoriamente.

Comprobación de carga de certificados en el almacén de Firefox

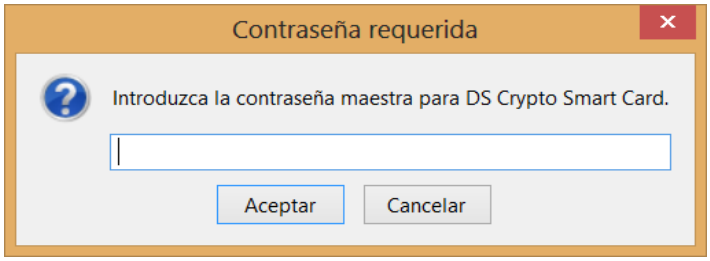
Si dispone en su máquina del explorador Mozilla Firefox en cualquiera de sus versiones realice también la siguiente prueba:

- Abra el menu desplegable *Herramientas* del menú superior
- Selecione opciones y vaya a la pestaña *Avanzado*
- Abra la pestaña Certificados



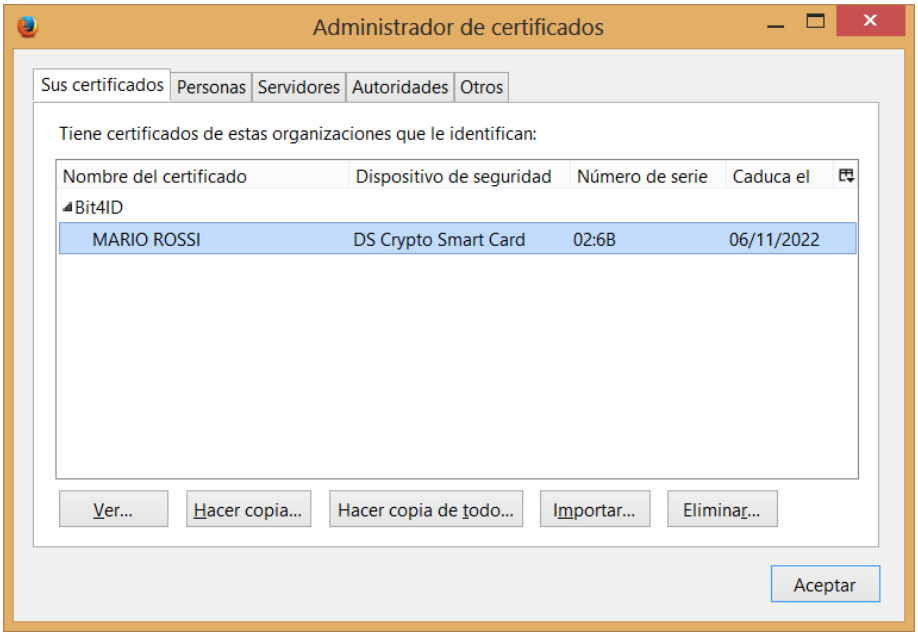
[Imagen 10]

- Ejecute la opción *Certificados* o *Ver certificados* (dependiendo de la versión del explorador)
- Introduzca el *PIN* de su tarjeta



[Imagen 11]

Una vez introducido el PIN, Vaya a la pestaña *Sus certificados* como muestra la siguiente imagen:



[Imagen 12]

Si se le muestra información referente a los certificados de su tarjeta la comprobación habrá finalizado satisfactoriamente.

NOTA: Además de los resultados de las comprobaciones expuestas en este apartado, indique al departamento técnico la versión del Kit Bit4id. Para conocer la versión de su kit siga las instrucciones expuestas en el siguiente apartado Preguntas Frecuentes, concretamente en la respuesta de la pregunta *¿Cómo puedo comprobar que dispongo de las últimas versiones del Kit Bit4id?*

Preguntas frecuentes

¿Qué puede ocurrir si, usando Card Manager, me aparece el mensaje de error "C_OpenSession debido al error 0x1"?

Consulte con el proveedor de la tarjeta (Autoridad de Certificación) sobre el estado de la misma, indicando todos los pasos que ha llevado a cabo.

¿Qué puede ocurrir si, usando Card Manager, me aparece el mensaje de error "C_Login debido al error 0x5"?

Es posible que el código PIN de su tarjeta se encuentre en un estado inconsistente. Pruebe a cambiarlo.

Si el error permanece, consulte con el proveedor de la tarjeta (Autoridad de Certificación) sobre el estado de la misma, indicando todos los pasos que ha llevado a cabo.

¿Qué puede ocurrir si al intentar cambiar el PIN de la tarjeta le aparece me el mensaje de error "C_SetPIN debido al error 0x6"?

Compruebe que el nuevo PIN tiene entre 6 y 8 dígitos alfanuméricos.

¿Puedo combinar números y letras para el número PIN de la tarjeta?

Sí, no hay ningún problema, siempre que el nuevo PIN tenga entre 6 y 8 dígitos.

¿Existe un máximo de inserciones de PIN en el caso de que tenga alguna duda y no recuerde mi número PIN? ¿Cuándo puede quedar bloqueada la tarjeta?

Si inserta más de 3 veces el código PIN de forma errónea, este se bloquea. Póngase en contacto con Bit4id para desbloquearlo.

¿Existe un máximo de inserciones de PUK para intentar desbloquear el PIN? ¿Qué ocurre si la tarjeta queda bloqueada?

Si inserta más de 3 veces el código PUK de forma errónea, este se bloquea. Por razones de seguridad, la tarjeta se bloquea completamente. Póngase en contacto con Bit4id.

¿Cómo puedo comprobar que dispongo de las últimas versiones del Kit Bit4id?

Para comprobar la versión instalada de forma sencilla en Windows XP, diríjase al menú Inicio > Panel de control > Agregar o quitar programas > Bit4id Card Manager Admin x.x.x.x (dónde x.x.x.x representa el número de versión instalada)

En Windows Vista o 7, diríjase al menú Inicio > Panel de control > > Desinstalar un programa > Bit4id Card Manager Admin x.x.x.x (dónde x.x.x.x representa el número de versión instalada)

En Windows 8, diríjase al menú lateral derecho > Configuración > Panel de control > Desinstalar un programa > Bit4id Card Manager Admin x.x.x.x (dónde x.x.x.x representa el número de versión instalada)

¿Qué puede ocurrir si al ejecutar el instalador del Kit Bit4id tengo una versión anterior instalada en el ordenador?

Siempre es recomendable eliminar versiones anteriores antes de instalar. No obstante, el instalador está diseñado para detectarlo automáticamente y eliminar versiones anteriores. Siga atentamente las instrucciones por pantalla.

Glosario

Autoridad de Certificación: Es la entidad de confianza, responsable de emitir y revocar los certificados electrónicos, utilizados en la firma electrónica. La Autoridad de Certificación, por sí misma o mediante la intervención de una Autoridad de Registro, verifica la identidad del solicitante de un certificado antes de su expedición o, en caso de certificados expedidos con la condición de revocados, elimina la revocación de los certificados al comprobar dicha identidad.

Caducidad del certificado digital: El certificado digital tiene un período de vigencia que consta en el mismo certificado. Generalmente es de 2 años, aunque por ley se permite una vigencia de hasta 5 años. Una vez el certificado haya caducado, no se podrán utilizar los servicios ofrecidos por la Administración que requieran firma electrónica, y cualquier firma electrónica que se haga a partir de ese momento no tendrá validez.

Certificado digital: Documento en soporte informático emitido y firmado por la Autoridad de Certificación, que garantiza la identidad de su propietario.

Certificado reconocido: Certificado expedido por un Prestador de Servicios de Certificación que cumple los requisitos establecidos en la Ley en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que presten, de conformidad con lo que dispone el capítulo II del Título II de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica.

Firma electrónica: Conjunto de datos, en forma electrónica, anejos a otros datos electrónicos o asociados funcionalmente con ellos, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge. Existen 3 tipos de firma electrónica: firma electrónica simple, avanzada y reconocida.

Firma electrónica simple: Conjunto de datos, en forma electrónica, anejos a otros datos.

Firma electrónica avanzada: Firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.

Firma electrónica reconocida: Se considera firma electrónica reconocida la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma. La firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.

Función hash: es una operación que se realiza sobre un conjunto de datos de cualquier tamaño, de forma que el resultado obtenido es otro conjunto de datos de tamaño fijo, independientemente del tamaño original, y que tiene la propiedad de estar asociado unívocamente a los datos iniciales, es decir, es imposible encontrar dos mensajes distintos que generen el mismo resultado al aplicar la Función hash.

Hash o Huella digital: Resultado de tamaño fijo que se obtiene tras aplicar una función hash a un mensaje y que cumple la propiedad de estar asociado unívocamente a los datos iniciales.

Integridad: La integridad es la cualidad que posee un documento o archivo que no ha sido alterado y que además permite comprobar que no se ha producido manipulación alguna en el documento original.

Listas de Revocación de Certificados o Listas de Certificados Revocados: Lista donde figuran exclusivamente las relaciones de certificados revocados o suspendidos (no los caducados).

No repudio: El emisor que firme electrónicamente un documento no podrá negar que envió el mensaje original, ya que éste es imputable al emisor por medio de la clave privada que únicamente conoce él y que está obligado a custodiar. El no repudio permite, además, comprobar quién participó en una transacción.

El no repudio o irrenunciabilidad es un servicio de seguridad estrechamente relacionado con la autenticación y que permite probar la participación de las partes en una comunicación. La diferencia esencial con la autenticación es que la primera se produce entre las partes que establecen la comunicación y el servicio de no repudio se produce frente a un tercero

Prestador de Servicios de Certificación o PSC: Persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica. Ver Autoridad de Certificación.

PIN: Secuencia de caracteres que permiten el acceso a los certificados. Número de Identificación Personal, en ocasiones llamado NIP.

PUK: Secuencia de caracteres que permiten el cambio o desbloqueo del PIN. Clave Personal de Desbloqueo.

Renovación: La renovación consiste en solicitar un nuevo certificado mediante un certificado vigente pero que está a punto de caducar. De esta manera, antes de la caducidad de un certificado se puede solicitar la renovación y esto implica que se emita un nuevo certificado válido.

Revocación: Anulación definitiva de un certificado digital a petición del suscriptor, o por propia iniciativa de la Autoridad de Certificación en caso de duda de la seguridad de las claves. La revocación es un estado irreversible. Se puede solicitar la revocación de un certificado después de una situación de suspensión o por voluntad de las personas autorizadas a solicitarla. De la misma manera, en el caso de un certificado suspendido, si ha pasado el periodo de suspensión máximo, si el certificado no ha sido habilitado, pasa a estar definitivamente revocado. Cuando la entidad de certificación revoca o suspende un certificado, ha de hacerlo constar en las Listas de Certificados Revocados (CRL), para hacer público este hecho. Estas listas son públicas y deben estar siempre disponibles.

Tarjeta inteligente (smartcard): Cualquier tarjeta con circuitos integrados que permiten la ejecución de cierta lógica programada.